Journal of Number Theory **84**, 34–39 (2000)
doi:10.1006/jnth.2000.2529, available online at http://www.idealibrary.com on IDEAL®

Continuous π-adic Functions and π-Derivations

Alexandru Buium

Department of Mathematics, University of New Mexico, Albuquerque, New Mexico 87131

Communicated by D. Goss

Received October 18, 1999; revised December 13, 1999

Let K be a local field, $\mathcal{O}$ the ring of integers of K, and π a uniformizer of $\mathcal{O}$. Assume ϕ is an automorphism of K lifting the q-power map on the residue field $\mathcal{O}/(\pi)$. (Such a ϕ exists, for instance, if K is a Galois extension of a finite extension k of $\mathbf{Q}_p$, and q is the size of the residue field of k.) Define $\delta: \mathcal{O} \to \mathcal{O}$ by

$$\delta(a) = \frac{\phi(a) - a^q}{\pi}.$$

We shall view δ as playing the role of a "derivative with respect to π" in the spirit of [B1], where such a δ is called a π-derivation. Note that ϕ and δ are not locally analytic maps (indeed, they are not even differentiable). Let Q be the size of the residue field of $\mathcal{O}$. (We do not assume $Q = q$ in general.) For a multi-index $\underline{i} = (i_0, i_1, i_2, \ldots)$ with integer coordinates satisfying $0 \leqslant i_j \leqslant Q-1$ and $i_j = 0$ for large j, write $|\underline{i}| = i_0 + i_1 + i_2 + \cdots$ and set

$$\delta_{\underline{i}}(a) = a^{i_0} (\delta a)^{i_1} (\delta^2 a)^{i_2} \ldots,$$

which really is a finite product. (So $\delta_{(1, 0, 0, \ldots)}(a) = a$ and $\delta_{(0, 1, 0, \ldots)}(a) = \delta a$.)

Our aim is to prove the following:

THEOREM. *Every continuous function $f: \mathcal{O} \to \mathcal{O}$ can be written in the form*

$$f(a) = \sum_{\underline{i}} c_{\underline{i}} \delta_{\underline{i}}(a)$$

for a unique sequence $c_{\underline{i}} \in \mathcal{O}$ which tends to 0 as $|\underline{i}| \to \infty$ and $|f|_{\sup} = \max_{\underline{i}} |c_{\underline{i}}|$.

Let $C(\mathcal{O}, \mathcal{O})$ be the space of all continuous functions from $\mathcal{O}$ to $\mathcal{O}$. By an *orthonormal basis* for $C(\mathcal{O}, \mathcal{O})$ one understands a family of functions in $C(\mathcal{O}, \mathcal{O})$ such that any function in $C(\mathcal{O}, \mathcal{O})$ is an infinite linear combination of the functions in the family, with coefficients in $\mathcal{O}$ that tend to 0, and the

0022-314X/00 $35.00

supremum norm of the function is the maximum absolute value of these coefficients. With this terminology, the result above says that the family of functions $a \mapsto \delta_i(a)$ is an orthonormal basis of $C(\mathcal{O}, \mathcal{O})$. This is analogous to Mahler's theorem [M, p. 51] stating that the binomial coefficient functions

$$a \mapsto \binom{a}{n} := \frac{a(a-1)\cdots(a-n+1)}{n!}$$

form an orthonormal basis of $C(\mathbf{Z}_p, \mathbf{Z}_p)$.

The functions $a \mapsto \delta_i(a)$ may be viewed as (non-linear) "differential operators" (relative to δ); since the "orders" of these operators generally go to ∞ in the representation of a given function f, the right hand side of the equality in the Theorem may be viewed as a (non-linear) "pseudo differential operator".

The case $\mathcal{O} = \mathbf{Z}_p$ of our theorem is known (see, for instance, [CC, p. 33]), and is actually easily seen to be equivalent to Mahler's theorem, as pointed out to us by F. Voloch. In case $\mathcal{O}$ is unramified over $\mathbf{Z}_p$ another orthonormal basis for $C(\mathcal{O}, \mathcal{O})$ is described in [CC, p. 33]; it consists of the iterates of the polynomial function $x \mapsto (x^Q - x)/p$. When $\mathcal{O} \neq \mathbf{Z}_p$ there does not seem to be an easy, direct relation between the orthonormal basis in [CC] and the one in the Theorem above.

An analogue in characteristic p of our result has been proved by Jeong and Snyder [JS]. Let $R = F[[x]]$, where F is a finite field with q elements, with R having the topology given by the usual valuation. Define the Hasse derivatives $D^{(r)}: R \to R$ by $D^{(r)}(\sum a_n x^n) = \sum \binom{n}{r} a_n x^{n-r}$, which are continuous F-linear functions. Jeong and Snyder prove that the collection of functions

$$a \mapsto a^{i_0} D^{(1)}(a)^{i_1} D^{(2)}(a)^{i_2} \cdots D^{(r)}(a)^{i_r},$$

where $0 \leqslant i_j \leqslant q-1$, is an orthonormal basis for $C(R, R)$. They also relate these differential operators to the Carlitz-Wagner functions which are the function field analogue of the binomial coefficients.

After the present paper was submitted the author received a preprint by K. Conrad [C] in which a general theory of orthonormal bases is developed, based on what the author calls "the digit principle"; in particular, our Theorem follows from [C, Theorem 3].

To prove our Theorem we need the following

LEMMA 1. *For any n, the map $\mathcal{O}/(\pi^{n+1}) \to (\mathcal{O}/(\pi))^{n+1}$ given by*

$$a \bmod \pi^{n+1} \mapsto (a, \delta a, ..., \delta^n a) \bmod \pi$$

is a bijection.

Proof. First, for any positive integer j and any $a, b, c \in \mathcal{O}$, one has

$$b \equiv a + \pi^j c \bmod \pi^{j+1} \Rightarrow \delta b \equiv \delta a + \pi^{j-1} u^j c^q \bmod \pi^j,$$

where $u = (\phi\pi)/\pi \in \mathcal{O}^\times$. By iteration this yields, for any $n \geqslant 1$ and any $i \leqslant n$,

$$\delta^i(a + \pi^n c) \equiv \delta^i a + \pi^{n-i} v c^{q^i} \bmod \pi^{n+1-i}$$

for some $v \in \mathcal{O}^\times$ that depends on a, c, i and n. Now to check Lemma 1, it is enough, for cardinality reasons, to check the injectivity of our map. We proceed by induction on n. Assume $a, b \in \mathcal{O}$ are such that $\delta^i a \equiv \delta^i b \bmod \pi$ for $0 \leqslant i \leqslant n$. By induction $b = a + \pi^n c$ for some $c \in \mathcal{O}$. Hence

$$\delta^n b = \delta^n(a + \pi^n c) \equiv \delta^n a + v c^{q^n} \bmod \pi$$

for some $v \in \mathcal{O}^\times$ so $c^{q^n} \equiv 0 \bmod \pi$, hence $c \equiv 0 \bmod \pi$ and we are done.

LEMMA 2. *Every map from $\mathcal{O}/(\pi^{n+1})$ to $\mathcal{O}/(\pi)$ can be written in the form*

$$a \bmod \pi^{n+1} \mapsto \sum_{i_0, \ldots, i_n = 0}^{Q-1} c_{i_0, \ldots, i_n} a^{i_0} (\delta a)^{i_1} \cdots (\delta^n a)^{i_n} \bmod \pi$$

for a unique sequence of coefficients $c_{i_0, \ldots, i_n} \in \mathcal{O}/(\pi)$.

Proof. For cardinality reasons it is enough to check that if such a function vanishes then all coefficients are 0. By Lemma 1, the corresponding polynomial function

$$g(x_0, \ldots, x_n) = \sum_{i_0, \ldots, i_n = 0}^{Q-1} c_{i_0, \ldots, i_n} x_0^{i_0}, \ldots, x_n^{i_n}$$

from $(\mathcal{O}/(\pi))^{n+1}$ to $\mathcal{O}/(\pi)$ is identically 0. Since the exponents are all at most $Q-1$, the coefficients all vanish.

Proof of the Theorem. The argument follows Serre's argument in [S, Lemma 1] closely. The "if" part is trivial. For the "only if" part we construct, by induction, a sequence $F_j \in \mathcal{O}[x_0, x_1, x_2, \ldots]$ of polynomials of degree $\leqslant Q-1$ in each variable and a sequence of continuous functions $f_j: \mathcal{O} \to \mathcal{O}$ $(j \geqslant 1)$ such that

$$\pi f_j(a) = f_{j-1}(a) - F_j(a, \delta a, \delta^2 a, \ldots)$$

for all $a \in \mathcal{O}$. (By convention we set $f_0 = f$, $F_0 = 0$.) This will finish the proof of the "only if" statement, for if

$$F = F_1 + \pi F_2 + \pi^2 F_3 + \cdots$$

then all monomials of F have degree $\leqslant Q-1$ in each variable and

$$f(a) = F(a, \delta a, \delta^2 a, \ldots)$$

for all $a \in \mathcal{O}$. Assume f_j, F_j are constructed for some $j \geqslant 0$. Since f_j is continuous there exists $n = n(j)$ such that the composition $\mathcal{O} \xrightarrow{f_j} \mathcal{O} \xrightarrow{can} \mathcal{O}/(\pi)$ factors through a map $\mathcal{O}/(\pi^{n+1}) \to \mathcal{O}/(\pi)$. Applying Lemma 2 to the latter map we find a polynomial $F_{j+1} \in \mathcal{O}[x_0, \ldots, x_n]$, of degree $\leqslant Q-1$ in each variable, such that

$$f_j(a) \equiv F_{j+1}(a, \delta a, \delta^2 a, \ldots, \delta^n a) \bmod \pi$$

for all $a \in \mathcal{O}$. We are done by setting

$$f_{j+1}(a) = (f_j(a) - F_{j+1}(a, \delta a, \delta^2 a, \ldots, \delta^n a))/\pi$$

for $a \in \mathcal{O}$. By construction, F has degree $\leqslant Q-1$ in each variable. To prove orthonormality we must check that if

$$F(a, \delta a, \delta^2 a, \ldots) \equiv 0 \bmod \pi$$

for all $a \in \mathcal{O}$ then all coefficients of F are divisible by π. Assume the contrary, so at least one of the coefficients is not divisible by π. Let $G \in \mathcal{O}[x_0, \ldots, x_n]$ be the sum of all monomials of F whose coefficients are not divisible by π. We have

$$G(a, \delta a, \ldots, \delta^n a) \equiv 0 \bmod \pi$$

for all $a \in \mathcal{O}$. But this contradicts Lemma 2, which closes our proof.

Let $\mathcal{O}\langle x_0, x_1, x_2, \ldots\rangle$ be the π-adic completion of the ring of polynomials in $x_0, x_1, x_2, \ldots$, with $\mathcal{O}$-coefficients. Any element $F \in \mathcal{O}\langle x_0, x_1, x_2, \ldots\rangle$ can be viewed as a restricted power series, i.e., a formal power series in $x_0, x_1, x_2, \ldots$ with coefficients tending to 0; therefore any such F can be evaluated at any sequence $a_0, a_1, a_2, \ldots \in \mathcal{O}$ to give an element

$$F(a_0, a_1, a_2, \ldots) \in \mathcal{O}.$$

Then our Theorem implies, in particular, that for any continuous map $f: \mathcal{O} \to \mathcal{O}$ one can find a restricted power series $F \in \mathcal{O}\langle x_0, x_1, x_2, \ldots\rangle$ such that

$$f(a) = F(a, \delta a, \delta^2 a, \ldots)$$

for any $a \in \mathcal{O}$. Our Theorem is more precise since it guarantees that F can be chosen (uniquely) such that all its monomials have degree $\leqslant Q-1$ in

each variable. Let us, however, allow now that the monomials of F have arbitrary degree; then the series F will cease to be unique. A priori F will depend on infinitely many variables. One can ask which continuous functions f are represented by F's that depend on finitely many variables only; morally, the question is which f's are "differential operators" rather than "pseudo differential operators."

Let us look at a "multiplicative analogue", and then at an "elliptic analogue" of this question. A trivial consequence of our Theorem is that for any continuous function $f: \mathcal{O}^\times \to \mathcal{O}$ there exists a (not necessarily unique) restricted power series $\Phi \in \mathcal{O}\langle x_{-1}, x_0, x_1, x_2, \ldots\rangle$ such that

$$f(a) = \Phi(a^{-1}, a, \delta a, \delta^2 a, \ldots)$$

for all $a \in \mathcal{O}^\times$. (Indeed, one way of seeing this is to define f on the whole of $\mathcal{O}$ by setting $f(a) = 0$ for $a \in \mathcal{O} \setminus \mathcal{O}^\times$ and then applying the Theorem to this extended f. In this way we can even choose Φ such that x_{-1} does not occur in it; however we want, in what follows, to allow that Φ depend on x_{-1} as well.) One can ask again which f's are representable by Φ's that depend on finitely many variables only? This question seems to be non-trivial even in case $\mathcal{O} = \mathbf{Z}_p$. An interesting example of an (actually locally constant!) $f: \mathbf{Z}_p \to \mathbf{Z}_p$ having this property plays a role in [B2]: it is provided by the Legendre symbol

$$f(a) := \left(\frac{a}{p}\right) = a^{(p-1)/2}\left[1 + \sum_{j \geqslant 1} \left(\frac{1/2}{j}\right) p^j \left(\frac{\delta a}{a^p}\right)^j\right].$$

Here we assume $p \neq 2$. Other examples can be given using higher power residue symbols. A natural question is then: which locally constant functions $f: \mathbf{Z}_p^\times \to \mathbf{Z}_p$ are representable by Φ's that depend on finitely many variables only? One can suitably generalize this question for functions of several variables; the reason why this is interesting is that the traces of Frobenii on an elliptic curve $y^2 = x^3 + ax + b$, $a, b \in \mathbf{Z}$, are expressible (in a certain precise sense, cf. [B2]) in terms of power series, with coefficients tending to 0, in a, b, δa, δb, $\delta^2 a$, $\delta^2 b$, $(4a^3 + 27b^2)^{-1}$. Does this "differential operator character" of the traces of Frobenii (as opposed to the "pseudo differential character" of arbitrary continuous functions) impose any restrictions on the traces of Frobenii?

ACKNOWLEDGMENTS

The author thanks Felipe Voloch and Keith Conrad for a series of discussions and comments on an earlier version of this paper. The author also thanks the NSF for support through Grant DMS 9996078.

REFERENCES

[B1] A. Buium, Differential characters of Abelian varieties over p-adic fields, *Invent. Math.* **122** (1995), 309–340.

[B2] A. Buium, Differential modular forms, *Crelle J.* **520** (2000), 95–167.

[CC] P. J. Cahen and J.-L. Chabert, "Integer Valued Polynomials," Mathematical Surveys and Monographs, Vol. 48, Amer. Math. Soc., Providence, RI, 1997.

[C] K. Conrad, The digit principle, *J. Number Theory*, to appear.

[JS] S. T. Jeong and B. Snyder, Hyper-differential operators and continuous functions on function fields, preprint.

[M] K. Mahler, "Introduction to p-adic Numbers and Their Functions," Cambridge Tracts in Math., Vol. 64, Cambridge Univ. Press, Cambridge, UK, 1973.

[S] J.-P. Serre, Endomorphismes complètement continus des espaces de Banach p-adiques, *Publ. Math. IHES* **12** (1962), 69–85.